CLAIMS

What is claimed is:

1. A method in a distributed system, comprising the steps of:

downloading code from a server;

determining a set of constraints to implement secure communication with the server; and

using secure code to verify that the downloaded code will enforce the set of constraints when the downloaded code is used to communicate with the server.

2. The method of claim 1, further comprising the step of:

using the downloaded code to invoke a method on the server, wherein the downloaded code enforces the set of constraints on the server.

3. A method in a distributed system for ensuring trustworthiness of a first proxy, comprising the steps of:

downloading the first proxy containing code for communication purposes;

using the first proxy to obtain a second proxy containing code for communication purposes;

determining whether the second proxy is trustworthy by using a trustworthiness verification routine;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

determining whether a server is trustworthy by using the second proxy when it has been determined that the second proxy is trustworthy;

requesting the server to determine whether the first proxy is trustworthy by using the second proxy when it has been determined that the server is trustworthy; and

using the first proxy to invoke a method on the server when it has been determined that the first proxy is trustworthy, that the second proxy is trustworthy, and that the server is trustworthy.

4. The method of claim 3, wherein the requesting step further comprises the substeps of:

receiving a trust verifier routine from the server;

receiving codebase information and signer information for the trust verifier from the server;

determining whether the trust verifier routine is trustworthy using the codebase information and the signer information; and

when it has been determined that the trust verifier routine is trustworthy, using the trust verifier routine to determine whether the first proxy is trustworthy.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

5. A method for establishing trust in a proxy containing code downloaded from a server, comprising the steps of:

determining whether the proxy is an instance of a trusted proxy class;

verifying at least one component of the proxy when it has been determined that the proxy is an instance of the trusted proxy class, wherein the verifying step comprises the substeps of:

verifying trust in an invocation handler of the proxy;

determining whether the proxy has an activator; and

verifying the trustworthiness of the activator, when it has been determined that the proxy has an activator; and

using the proxy to invoke a method on the server when it has been determined that the proxy is an instance of the trusted class and the at least one component of the proxy has been verified successfully.

6. A method for establishing trust in a proxy containing code downloaded from a server, comprising the steps of:

determining whether the proxy is an instance of a trusted proxy class;

verifying at least one component of the proxy when it has been determined that the proxy is an instance of a trusted proxy class, wherein the proxy has an invocation handler and a plurality of socket factories, and wherein the verifying step comprises the substeps of:

obtaining the invocation handler from the proxy;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

testing whether the invocation handler is an instance of a secure invocation handler class;

comparing a class of each socket factory of the invocation handler to a list of trusted socket factory classes;

setting an error flag if the class of any socket factory of the invocation handler does not match the list of trusted socket factory classes;

determining whether the proxy has an activator; and

authenticating the activator, when it has been determined that the proxy has an activator, wherein the authenticating step further includes the substeps of:

obtaining an activator verifier from the server;

using the activator verifier to determine whether the activator is trusted by the server; and

setting the error flag, when it is determined that the activator is not trusted by the server; and

using the proxy to invoke a method on the server when the error flag is not set and when it has been determined that the proxy is an instance of the trusted class.

7. A distributed system comprising:

a server computer, comprising:

a memory with a service; and

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

a processor that runs the service; and

a client computer, comprising:

a memory with a proxy that facilitates use of the service, a client program that invokes a method of the service using the proxy, and a secure verifier that can be used to verify that the proxy will enforce security constraints when communicating with the service; and

a processor that runs the client program.

8. The distributed system of claim 7, wherein the server computer and the client computer communicate via the Internet.

9. The distributed system of claim 7, wherein the server computer and the client computer communicate via a local area network.

10. The distributed system of claim 7, wherein the security constraints are set by the client program.

11. The distributed system of claim 7, wherein the security constraints are set by the service.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

12. A computer-readable medium containing instructions for controlling a data processing system to perform a method in a distributed system, the method comprising the steps of:

downloading code from a server;

determining a set of constraints to implement secure communication with the server; and

using secure code to verify that the downloaded code will enforce the set of constraints when the downloaded code is used to communicate with the server.

13. The computer-readable medium of claim 12, wherein the method further comprises the step of:

using the downloaded code to invoke a method on the server, wherein the downloaded code enforces the set of constraints on the server.

14. A computer-readable medium containing instructions for controlling a data processing system to perform a method in a distributed system the method comprising the steps of:

downloading the first proxy containing code for communication purposes;

using the first proxy to obtain a second proxy containing code for communication purposes;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

determining whether the second proxy is trustworthy by using a trustworthiness verification routine;

determining whether a server is trustworthy by using the second proxy when it has been determined that the second proxy is trustworthy;

requesting the server to determine whether the first proxy is trustworthy by using the second proxy when it has been determined that the server is trustworthy; and

using the first proxy to invoke a method on the server when it has been determined that the first proxy is trustworthy, that the second proxy is trustworthy, and that the server is trustworthy.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000